

METHOD AND SYSTEM FOR SECURELY HANDLING  
INFORMATION BETWEEN TWO INFORMATION PROCESSING DEVICES

BACKGROUND OF THE INVENTION

5

Technical Field

10

The present invention generally relates to secure interoperation between two information processing devices where only one of these devices can handle information in a secure manner. In particular, the present invention relates to a method and a system for securely handling an information unit by a first information processing device, for instance a terminal device, interoperating with a second secure information processing device, for instance a portable device like a chip card, whereby the information unit is provided by an issuer.

15

Prior Art

20

It is commonly known that chip cards are not only utilized as a memory for storing data on it but also used as an access control medium or a medium to enable and perform encryption and decryption of information. Therefore, from the beginning of development of chip cards, the field of cryptology has played a central or even dominant role. Meanwhile, the scientific results of this development field are inseparably related to chip card technology.

25

30

The technical field of cryptology divides into two fields of activity, namely cryptography and cryptanalysis, The field of cryptography embraces the science and methodology of encryption and decryption of information.

The science of cryptanalysis addresses to crack existing cryptographic systems.

5 In the field of chip card technology, another major issue is practicability of the scientific and theoretical aspects of cryptology.

10. The predominant objective of cryptology is, on the one hand, secrecy of information and, on the other hand, securing or safeguarding the authentication of information. Both objectives are independently of each other and thus have different requirements of the respective information system. 'Secrecy' means that only the addressed receiver is able to decrypt the contents of a message. In contrast to that, 'authenticity' enables the receiver of the message to secure that the received message has not been altered during transmission.

20 For the following description of known techniques of data encryption/decryption it is referred to chapter 4 of the "Handbuch der Chipkarten", W. Rankl, W. Effing, 1996, Hauser Verlag, Munich-Vienna, which contents are regarded to be fully incorporated herein. Each encryption technique uses three types of information. Non-encrypted data are designated as "plain text" wherein encrypted data are designated as "cypher text". For encryption/decryption one or more keys are required as third type of data. All these types of data are to be processed by an encryption algorithm. Cryptographic algorithms currently used in chip cards are generally block-oriented, which means that the plain text and the cypher text are always processed as packages of a given

length, e.g. 8 byte in case of the algorithm used by the decryption/encryption standard (DES) which is discussed in more detail in the following.

5 It is emphasized hereby that the present invention is applicable to all described fields of cryptography like encryption, decryption, or one-way cryptographic functions like hash values or digital signature verification mechanism. Modern cryptographic algorithms  
10 are generally based on the known Kerckhoff principle which says that the entire security of an algorithm shall only depend on secrecy of the underlying keys, but not on secrecy of the cryptography algorithm itself.

15 Besides Kerckhoff, a further known principle is security through masking which presumes that a fictitious attacker does not know how the system works. But the latter principle is by no means sufficient to secure an information handling system. The security of modern and  
20 already published cryptographic algorithms does, in practice, only depend on the performance of the computers used to crack a cryptographic algorithm and thus an alleged additional masking technique of the utilized methodology of crypton one achieves a considerably  
25 increased protection against attacks. Otherwise, the rapidly progressing development of computer performance causes a doubling of performance within about one and a half years and thereupon the increasing number of participants of the worldwide computer network, e.g. the  
30 WEB, provide a further way to perform serious attacks on cryptographic systems or related keys.

In order to crack a cryptographic algorithm, there are different ways of attacks. A first one is the "cypher text only attack" where the attacker does only know the cypher text and tries to obtain the key or plain text by use of this information. A more promising attack is the so-called "known plain text attack" where the attacker is in the possession of a number of plain-text/cypher-text pairs for a secret key. The secret key can be obtained by trial and error. The most trivial attack is to find out the secret key only through trial and error which is called "brute force attack". By using a large performance computer, on the basis of a known plain-text/cypher-text pair, all feasible encryption keys are tried until the right one is obtained. The teaching of statistics says that on an average only the half of all possible keys has to be checked in order to find the right one. For that reason, a large space of possible keys renders that kind of attack more difficult.

Cryptographic algorithms are further divided into symmetric and asymmetric algorithms, dependent on the respectively utilized key. 'Symmetric' means that algorithm for en- and decryption is using the same key. In contrast to that, 'asymmetric' cryptographic algorithms, like that proposed by Whitfield Diffie and Martin E. Hellman in 1976, are using different keys for encryption and decryption. The two major principles for a well performing encryption algorithm are the principles of 'confusion' and 'diffusion' after C. Shannon. It is emphasized that both types of algorithms can be taken as a basis for the present invention.

Symmetric cryptographic algorithms are based on the principle of utilizing the same key for both encryption and decryption. A well-known data encryption algorithm called 'Data Encryption Algorithm' (DEA) has been  
5 proposed by the applicant of the present application together with the U.S. National Bureau of Standards developed in 1977. This standard algorithm is often be referred to as 'Data Encryption Standard' (DES). Since that algorithm is designed in consideration of  
10 Kerckhoff's dogma, it could be published without any impact on its security. For the details of that algorithm it is further referred to National Institute of Standards and Technology (NIST), FIPS Publication 46-2, "Data Encryption Standard", December 1993.

15 The principle of 'confusion' means that the statistics of the cypher text shall influence the statistics of the plain text so that an attacker can not take profit by that. The second principle "diffusion" means that every  
20 bit of the plain text and of the key shall influence as much bits of the cypher text as possible.

25 The DEA is a symmetric encryption algorithm using block architecture. It does not perform expansion of the cypher text which means that plain text and cypher text are of identical length. The block length is 64 bit (=8 byte), the key is also 64 bit long but includes 8 parity bits whereby the available space of possible keys is considerably reduced which is in case of DES  $2^{56} = 7.2 \times 10^{16}$  possible keys. But in view of the continuously and  
30 permanently increasing computer performance such a space

of possible keys is regarded as the lower limit for the required security of a cryptographic algorithm.

As an exemplary asymmetric cryptographic algorithm, it is referred to the one proposed by Whitfield Diffie and Martin E. Hellman, published in 1976, which is based on two different keys. One of these keys is public, the other is secret. An information or message is encrypted by using the public key prior to transmission of an information and only the owner of the secret key is enabled to decrypt again the encrypted message. In particular, that principle for the first time enables implementation of a digital signature which in principle can be verified by everyone who is in the possession of the required (public) key. Exemplarily, it is referred to a first implementation of the prementioned principle for asymmetric cryptographic algorithms, namely the 'RSA' algorithm proposed by Ronald L. Rivest, Adi Shamir and Leonard Adleman which is the currently best known and most versatile asymmetric cryptographic algorithm. Its functional principle is based on the arithmetic of big integer numbers. Both keys are generated based on two big prime numbers. Encryption and decryption can be mathematically expressed by a modulo function, namely in case of encryption  $y = x^e \bmod n$ , for decryption  $x = y^d \bmod n$  with  $n = p \times q$  wherein  $x$  = plain text,  $y$  = cypher text,  $e$  = public key,  $d$  = secret key,  $n$  = public modulus and  $p$ ,  $q$  = secret prime numbers.

For the further details of an implementation of the RSA algorithm it is accordingly referred to R.L. Rivest, A. Shamir, and L.M. Adleman "A Method for obtaining Digital

Signatures and Public-Key Cryptosystems", Communications of the ACM, 21(2), pages 120-126, February 1978.

5 In addition to secrecy of information, another paradigm for encryption algorithms is 'authenticity' of a received message of information. As mentioned above, authenticity means that a message is not altered e.g. not manipulated. For that purpose, to the actual message a message authentication code is appended and both parts are  
10 transmitted to the receiver. The receiver is enabled to calculate its own message authentication code (MAC) and compares that code with the received code. In case of both matching, it is secured that the transmitted message has not been altered during transmission. For generating  
15 a MAC, a cryptographic algorithm with one secret key which is known to both communication partners is utilized. For the calculation of a MAC in principle every cryptographic algorithm can be used, but in practice, the above mentioned DEA algorithm is utilized  
20 nearly exclusively.

25 A particular scenario for the present invention is a situation where a chip card is inserted in a chip card acceptance device - in the following called "terminal device" - which does not yet have a support module capable of accessing the card or to fulfill a particular function of the chip card on the terminal. Therefore it is required to obtain the missing software component from an other source of information e.g. to download such  
30 required module from a central server connected to the internet. It is noted that the terminal device can either be a computer, like a personal computer or network

computer with a chip card reader/writer hardware, or a specialized device combining the chip card reader/writer hardware with an embedded computer.

5 The transmission will often take place over a network that is open to attacks. It is known that the chip card hereby ensures that the software component in the device accessing the chip card shares a secret to the chip card by using mechanisms called external authentication or  
10 challenge/response. Further, it is known that a digital signature secures the download of software but the public keys of all potential senders have to be stored on the hard disk of the computer. Therefore, it is necessary that it can be ensured that the software was not altered  
15 on its way through the network and that the software was sent by the owner of the public key. But getting the public key for signature verification must also be done in a secure way, before the download is secure. This requires a chain of certification authorities.

20 On the other hand, an authentication mechanism is needed to verify that the obtained software component is the most recent issued release of that software. Today, the version control is handled by continuously increasing a  
25 version number.

#### SUMMARY OF THE INVENTION

It is therefore an object of the present invention to provide a method and a system for securely interoperating  
30 a first information processing device, in particular a terminal device like a chip card reader, and a second secure information processing device, in particular a



portable device like a chip card, where the first device does not yet have an information unit like a software component required for interoperating the first and the second device like providing or controlling access to the second secure device. It is therefore required that the missing information unit is obtained from an other source of information. A particular object of the invention which is strongly related to the above object is that gathering the missing information unit is to be accomplished in a secure manner.

In order to solve the above objects and to avoid the above-mentioned drawbacks of existing mechanisms and systems, the invention proposes that the information unit is provided from the issuer to the first information processing device whereby the information unit is processed by a cryptographic process i.e. for instance encrypted and/or signed by a signature. The required key for the cryptographic process is particularly provided on the second secure information processing device. The information unit is cryptographically reprocessed i.e. for example decrypted and/or its signature verified by using the key. It is emphasized that the information unit can be secured by alternatively using encryption/decryption and signature verification or by using both mechanisms in parallel.

#### BRIEF DESCRIPTION OF THE DRAWINGS

Preferred embodiments of the present invention will now be described, by way of example only, with reference to the accompanying drawings in which:

Fig. 1 a schematic view of a preferred embodiment of the invention together with the underlying data flow;

5 Fig. 2a a flow diagram illustrating a method for encryption/decryption according to the invention;

Fig. 2b a flow diagram according to Fig. 2a in a case of a signing/signature verification.

10- DETAILED DESCRIPTION OF THE INVENTION

According to a first preferred embodiment, the information unit is provided from the issuer to the first information processing device whereby the information unit is encrypted by using a first key which is also provided in an encrypted format by using a second key. The second key is provided on the second secure information processing device and interconnecting the first information processing device and the second secure information processing device therefore enables to decrypt the first key by using the second key. By using the decrypted first key, the information unit can also be decrypted.

According to a second preferred embodiment of the invention, the information unit is provided from the issuer to the first information processing device whereby the information unit is signed by using a signature. The signature is provided from the issuer to the first information processing device whereby the signature is generated by using at least one key. Further the at least one key for signature verification is provided on the second secure information processing device. After

the first information processing device and the second secure information processing device have been interconnected, the at least one key for signature verification is transferred from the second secure information processing device to the first information processing device. Finally the signature of the information unit is verified by using the at least one key.

19. It is noteworthy that the information unit can be any set of (pure) data or an executable code like an application program or a hardware driver to run on the second secure device and/or the other device(s), i.e. any kind of information. Further the information unit can serve to run specific functions of the second secure device on the first device or on at least a third device attached to the first device. In particular, the information unit can provide an access control for the second secure device. Further, the second secure information processing device can be any device where the issuer of that device, and of the information unit, can secure that the private key "i" is secure and not alterable, i.e. securely stored on the device. Exemplary devices are chip cards, in particular smart cards, Personal Computers with an according access control, or any other portable devices like laptops, palmtops, organizers, etc. Accordingly, the first information processing device can be any device with which the second secure device can interoperate like a card accepting device, e.g. a card reader, or even a computer with a card accepting device attached thereto.

In particular, according to the invention, the second secure device provides the second key by which the first key has been encrypted and therefore interconnecting the first device and the second device enables firstly to  
5 decrypt the first key by using the second key and, secondly, to decrypt the information unit by using the decrypted first key. The basic concept of the invention therefore is to have the private (second) key securely stored on the second secure information processing device  
10 what guarantees that this key will remain private i.e., can not be gathered by a third party.

In case of a chip card and a chip card accepting device, the invention particularly enables dynamic secure  
15 download and execution of a missing software support, for instance support needed for specific functions of a chip card on a device attached to the chip card acceptance device. The software component can only be decrypted by the usage of a key "T". This key is transmitted in an encrypted form as key " $T_i$ " together with the software encrypted with it. Key " $T_i$ " can only be decrypted by the  
20 chip card knowing the key "I" that was used to encrypt the key "T". The key "I" is stored on the chip card by the issuer at the time of card issuing. One of the advantages of this procedure is that the issuer of the  
25 card can secure that the key "I" is a private key insofar as it is guaranteed that the key is not known by others. Further, any laterly required software support for the chip card can be secured by using this key. On the other  
30 hand, the session key "T" which maybe will be known by others through transfer to the terminal device, can be changed by the issuer from session to session thus

considerably enhancing data security. To make the card  
decrypt key " $T_i$ " using key "I", a command (APDU) is  
passed to the chip card that was transmitted together  
with the software module to be decrypted and used. In  
5 other words, the chip card which may be controlled by the  
downloaded software, itself plays a critical role in  
securing the integrity of the driving software. Insofar,  
the chip card itself retrieves the key T which has been  
used to encrypt the downloaded software via decryption of  
10 the encrypted key  $T_i$ . To prevent alteration of the  
transmitted software module, it is proposed that it will  
be encrypted or signed with one of the standard  
algorithms described in the introductory part. The issuer  
of the software has the required encryption, decryption  
15 or signature keys. Instead of requiring the terminal  
device to store and retrieve the matching decryption key  
or fetch the matching certificate, the present invention  
describes a way of using the chip card itself to retrieve  
that key. The chip card advantageously is the most secure  
20 and most convenient way to store the secret decryption  
key or the certificate or the card issuer. In this way,  
only software that is certified by the card issuer should  
be allowed to access the card.

25 It is emphasized that beyond encryption/decryption the  
invention can also employ digital signing or digital  
signature verification for the encryption by using the  
first key and/or the second key. For this signature case,  
the described mechanism provides a trusted way to the  
30 issuer's public signature key without the requiring  
complex certificate handling including chains of trust.

5 The information unit can advantageously be a program  
module or data to control access to a portable device by  
the terminal device, the integrity of the information  
unit hereby playing a rather critical role for data  
security. Further, the information unit can be an  
application program which can run either on the portable  
device or the terminal device or can serve to run  
specific functions of the portable device on the terminal  
device or on a second device attached to the terminal  
10 device. Also in these cases, data integrity plays a  
dominant role.

15 Portable devices like chip cards commonly provide only  
limited resources for processing data and according  
limited space for storing data. Therefore, according to  
another embodiment of the invention, both the decryption  
of the first key and the decryption of the information  
unit are accomplished on the terminal device's side.

20 In order to provide a more powerful and automatically  
operating system, according to another embodiment of the  
invention the first device provides a control command  
(APDU) to the second secure device which initiates or  
triggers the transfer of the second key to the first  
25 device, or initiates or triggers the beginning of  
decryption of the first key by using the second key.  
Hereby an operating system or program of the first device  
advantageously must not know how to decrypt key "T<sub>i</sub>" and  
can be freed from performing the decryption procedure.  
30 The first device only passes the APDU command to the  
second secure device. This embodiment enables that the  
entire procedure proposed by the invention can be

performed in the background i. e. not visible to the user whereby in particular the required second key is transferred to the first device without any needed interaction by the user.

5

In a preferred embodiment of the invention, the encrypted information unit and the encrypted first key are downloaded from a central server, e.g. a server interconnected with the Internet, particularly from a server provided by the issuer of the second secure device. Alternatively, the above mentioned control command can be downloaded, too, from such a server. In view of the continuously increasing meaning of the Internet, such kind of software support via download is a preferred way to obtain a required information unit.

10-  
15

In a further preferred embodiment of the invention, the second key required to decrypt the first key is securely stored on the second secure device at time of its issuing by the issuer. Since the issuer of the card will often be identical with the issuer of the information unit, it is hereby guaranteed that the second key will be compatible with the encryption of the first key.

20

According to a further embodiment of the invention, a third key can be used for authentication or version control of the underlying information unit. Hereby the second secure device contains a version number and a key "E" which the downloaded information unit accessing the second secure device must know. To prove that the information unit has the matching key "E", a challenge/response mechanism ("external authentication")

25

30

is used. This allows the issuer of the second secure device by changing the key "E" on that device, in combination with the other steps of the proposed mechanism, to initiate the second secure device and/or the first device to download a new version of the underlying information unit.

Using such a third key, it is possible to realize a further automatization of the proposed mechanism where the first device is initiated to download a new release of the information unit.

The proposed arrangement of the two different key levels enables, in accordance with another preferred embodiment of the invention, that the first key can be randomized between different sessions of interoperating the first and the second device, i. e. the issuer of the second secure device every time can use another random key T to encrypt the information unit with the cryptographic function. Therefore, it is advantageously not compromising the security that the key T is given back from the second device to the first device in a clear form.

It is emphasized again that the method and system according to the invention can be applied to signing and signature verification accordingly.

Further features, details and advantages of the present invention will become evident from the following detailed description of embodiments of the invention and the corresponding accompanying drawings,



Fig. 1 depicts a scenario where a chip card 1 is inserted in a chip card reader 2 which does not yet have a required software component capable of accessing the chip card 1. Therefore the operating system of the card reader 2 initiates that the missing software component be downloaded 3 from a central server 4 to the card reader 2. In order to validate that the downloaded software component was certified by the issuer and has not been altered in the meantime, in accordance with the invention, the following mechanism is proposed. The issuer's certificate and corresponding private key "I" is stored on the chip card 2 at the time the card is issued. Prior to the software download 3, an encryption with a session key "T" is applied to the underlying software component. The downloaded data therefore contains the cyphered software plus key "T<sub>i</sub>", i. e. the key "T" encrypted by a key "I", plus a command (APDU) to trigger or to make the chip card 1 decrypt key "T<sub>i</sub>". The APDU command, when sent to the chip card 1, results in a decryption of the key "T<sub>i</sub>" to reveal key "T" that was used to encrypt the software component. Due to the above-mentioned combination of two different key levels, the card issuer can every time change key "T" by another random key to encrypt the service with the cryptographic function. Therefore, it is not compromising the security that the key "T" is given back from the chip card 1 to the card reader 2 (terminal device) in clear form. The software module, in this embodiment, is to drive the terminal device 2 to access the chip card 1, but such a software module can also be an application program to run on either the chip card 1 or the terminal device 2 or fulfill specific functions on

the terminal device 2 or another (optional) device 5  
connected or attached to the terminal device 2. The  
device 5 can be part of the terminal device and can be  
any information handling device or system, or only part  
of such a system like a video display or the like.  
Normally the terminal device 2 will be a non-intelligent  
card accepting device and the device 5 an intelligent  
card reader. Further, the software module can be a driver  
to drive the chip card or an instrument to control access  
to the chip card itself.

It is emphasized that the functionality of the terminal  
device as proposed by the invention can be implemented by  
means of common memory and processor hard- and software  
components.

The underlying encryption/decryption process consists of  
the following steps. The information unit  $s$  is encrypted  
by using the key "T" and the key "T" is encrypted by  
using key "I" as follows:

$$\begin{aligned}x &= \text{enc}(s, T); \\ T_i &= \text{enc}(T, I).\end{aligned}$$

Both " $x$ " and " $T_i$ " are transferred from the central server  
4 to the card reader 2. The card reader 2 then instructs  
the chip card 1 to decrypt " $T_i$ " using "I":

$$T = \text{dec}(T_i, I).$$



(support module +  $T_i$  + APDU) can be downloaded as one file, e. g. in a compressed format using known compression tools like "WINZIP" or "PKZIP".

5 Then the 'APDU' control command is sent 26 to the chip card in order to initiate or to trigger the chip card to decrypt 27 the encrypted key " $T_i$ " by using key "I". Alternatively the chip card can be initiated to transmit the key "I" to the card reader and the decryption of " $T_i$ " performed by the card reader. In case the chip card 10- fulfills the decryption, the decrypted key "T" will be transferred back 28 to the card reader and then the support module be decrypted 29 by an operating system or program available on the card reader, by using the key 15 "T". The resulting decrypted support module then will be executed 23 by the card reader.

In case of an underlying signature/signature verification, the mechanism proposed by the invention 20 consists of the following steps. The information unit "s" is signed by using a signature key "I":

$$x = \text{sign}(s, I_{\text{priv}}).$$

25 Both "x" and "s" are transferred from the central server 4 to the card reader 2. The card reader 2 then gathers the key "I" for signature verification from the chip card 1 and performs the following signature verification operation:

$$\text{signver}(s, x, I_{\text{pub}}) == \text{OK} ?$$



card, and that the version of the software is appropriate.

Thereupon it is secured that the code can only be executed if it was certified by the issuer of the card, the issuer can make sure that the software accessing the card does not make any operations that can insecure the system like sending data to somebody else or logging data.

For a version control, the following step can be added to the sequence of steps depicted in either Fig. 2a or Fig. 2b:

External authentication with key "E" in order to verify that the version of the software module matches the smart card.

Authentication is herein regarded as any process through which one proves and verifies certain information. A chip card commonly uses external authentication to establish the identity of the terminal. This is done by ensuring that the terminal device shares a secret with the chip card.

An external authentication starts with the chip card wondering about the terminal's identity and sending a challenge - for example a random 8-byte sequence - to the terminal whose identity is being questioned. The terminal receiving the challenge encrypts it with its secret, a particular key, and sends back the encrypted result. The chip card now decrypts the encrypted message using the

key it knows the terminal possesses if it is authentic.  
If the message decrypts satisfactorily, i. e. the  
decrypted challenge is identical to the challenge  
originally sent by the chip card, then the chip card  
5 knows that the terminal possesses a particular key and  
this establishes its identity.

While the invention has been particularly shown and  
described with respect to preferred embodiments thereof,  
10 it will be understood by those skilled in the art that  
the foregoing and other changes in form and details may  
be made therein without departing from the spirit and  
scope of the invention.

15